

2011 Student Netbook Manual

1. College ICT policies and documents

- 1.1 – Consent Form for a Student Loan of a College Owned Netbook Computer (pg 2)
- 1.2 – Terms and Conditions for a Student Loan of a College Owned Netbook Computer (pg 4)
- 1.3 – Student ICT Acceptable Use Policy (pg 7)
- 1.4 – Student ICT Essential Competency Checklist (pg 9)

2. Features of the Acer Aspire One Netbook

- 2.1 – General specifications (pg 10)
- 2.2 – Preloaded software (pg 10)

3. Personalising your netbook

- 3.1 – Identification tag and label (pg 11)
- 3.2 – Logging in for the first time (pg 11)
- 3.3 – Creating a logical file structure (pg 11)
- 3.4 – Backing up your data (pg 12)
- 3.5 – Installing additional software (pg 12)
- 3.6 – Installing printers (pg 13)
- 3.7 – Setting up Outlook - optional (pg 13)
- 3.8 – Changing your settings for use at home (pg 17)
- 3.9 – Making use of Wi-Fi hotspots (pg 21)



4. Taking care of your netbook

- 4.1 – Transporting and storage (pg 25)
- 4.2 – Recharging the battery (pg 25)
- 4.3 – Cleaning your netbook (pg 25)
- 4.4 – Seeking support (pg 25)

5. Cybersafety (includes tips for parents)

- 5.1 – Cyberbullying (pg 26)
- 5.2 – Sexting (pg 27)
- 5.3 – Online grooming (pg 28)
- 5.4 – Protecting personal information (pg 29)
- 5.5 – Excessive internet usage (pg 30)





Catholic College Sale

Consent Form for Student Loan of a College Owned Netbook Computer

Agreement by Parent/Guardian

1. I consent to the College issuing my child with a netbook for use throughout the 2011 school year.
2. I have attended the **Parent Student ICT Forum** held at the Bishop Phelan Stadium at 7.00 pm on Wednesday 23 February 2011.
3. I have visited and made myself familiar with the information presented on the **Cybersmart** website (www.cybersmart.gov.au).
4. I have read and agree with the principles outlined in the **Student ICT Acceptable Use Policy**.
5. I have read and understand the need for my child to develop/maintain the skills described in the **Student ICT Essential Competency Checklist**.
6. I have read and agree to the **Terms and Conditions for Student Loan of a College Owned Netbook Computer**, including the section given below:

Warranty repairs shall be undertaken by the College at no cost to the student or their parents/guardians. However, parents/guardians shall be solely responsible for the cost of all non-warranty repairs (breakage, loss or theft). Repaired netbooks shall not be returned to the student until the repair cost charged by the College has been paid in full by their parents/guardians.

Parent/Guardian Name:

Parent/Guardian Signature:

Date:

Agreement by Student

1. I have attended the **Parent Student ICT Forum** held at the Bishop Phelan Stadium at 7.00 pm on Wednesday 23 February 2011.
2. I have visited and made myself familiar with the information presented on the **Cybersmart** website (www.cybersmart.gov.au).
3. I have read and understand my responsibilities as outlined in the **Student ICT Acceptable Use Policy**.
4. I am committed to develop/maintain the skills described in the **Student ICT Essential Competency Checklist**.
5. I have read and agree to the **Terms and Conditions for Student Loan of a College Netbook Computer**, including the section given below:

When attempting to rectify any netbook hardware or software issues the ICT Support Centre will begin by wiping the machine clean. Students should regularly back up their data onto an external hard drive or other form of secondary storage.

Student Name:

Student Signature:

Date:



Catholic College Sale

Terms and Conditions for Student Loan of a College Owned Netbook Computer

1. **Parties to Whom these Terms and Conditions Apply**

These terms and conditions apply to the student intended to be issued with a College owned netbook computer and their parent/guardian. A College netbook will not be issued to the student until these terms and conditions have been accepted by both the student and their parent/guardian.

2. **Ownership**

The College owns the netbook and loans it to the student. The netbook remains the property of the College at all times throughout the loan period. Neither the student or their parent/guardian shall have any ownership rights or title in the netbook and the student shall not at any time loan, assign, give away, dispose of, encumber or otherwise do anything to infringe on the College's ownership of the laptop.

3. **Purpose**

Loan of the netbook is for the exclusive use of the student in support of their learning.

4. **College Policies**

The student agrees to fully support the College in the implementation of rules, policies and procedures relating to student use of netbooks as documented in the College Website and Student Planner.

5. **Modifications**

The netbook configuration, hardware and software shall not be altered or modified in anyway by any person other than the College ICT Support Centre. Installation of any additional software should have an educational purpose.

6. **Repairs and Replacements**

All netbook repairs/replacements should be arranged through the ICT Support Centre immediately in the event that it is not operating correctly, any part of it is broken, it sustains any form of damage or is missing.

Warranty repairs/replacements shall be undertaken by the College at no cost to the student or their parents/guardians. However, parents/guardians shall be solely responsible for the cost of all non-warranty repairs/replacements (breakage, loss or theft). Repaired/replacement netbooks shall not be returned to the student until the repair/replacement cost charged by the College has been paid in full by their parents/guardians.

When attempting to rectify any netbook hardware or software issues the ICT Support Centre will begin by wiping the machine clean. Students should regularly back up their data onto an external hard drive or other form of secondary storage.

7. Annual Maintenance

The Student is required to return the netbook to the College ICT Support Centre at the end of the school academic year for annual maintenance. All data will be wiped clean. Students should regularly back up their data onto an external hard drive or other form of secondary storage.

8. Netbook Care

Students are responsible for care of the netbook. The student shall at all times take responsible care of the netbook and not expose it to undue risk of damage or theft. When transporting the netbook it should be carried in the protective case provided. The student will ensure the netbook is recharged at home each night.

9. Netbook Insurance

The netbook is not insured by the College for loss or theft. Loss or theft of the netbook is to be reported to the student's pastoral teacher and the College ICT Support Centre immediately. A replacement netbook will be issued to the student at the cost of the parent/guardian where return of the missing netbook is unlikely. For this reason, it is highly recommended that parents/guardians consider insuring the netbook as part of their Home & Contents Insurance.

10. Term of the Loan

The netbook loan commences when the student is issued with a College netbook and ends at the end of the academic year. The College may terminate the netbook loan, without notice, if in the opinion of the College, there is a serious breach of these terms and conditions or any related College policies.

11. Return of the Netbook

When the term of the netbook loan expires, or is terminated the student shall immediately return the netbook to the College ICT Support Centre. If, in the opinion of the College ICT Support Centre, the netbook is not in good working order and condition, parents/guardians will incur the cost of all non-warranty repairs. If the netbook has not been returned to the College ICT Support Centre within seven days of expiration of the netbook loan, parents/guardians will bear the full cost to replace the netbook.

12. College not Liable

The College is not responsible in any way and shall not be liable for any loss, cost or damage relating to the student netbook for the duration of the student loan.

13. Payment Terms

Any amount payable to the College by the parents/guardians pursuant to these Terms and Conditions are payable within 7 days of request by the College.

14. Changes to Terms and Conditions

These terms and conditions may be updated or amended by the College from time to time. The College shall communicate any such updates or amendments to students and parents/guardians via direct communication and/or the College website



Catholic College Sale

Student Information Communication Technologies (ICT) Acceptable Use Policy

Rationale

The purpose of this policy is to clarify what constitutes acceptable and unacceptable student use of Information and Communication Technologies (ICT). The College embraces student use of ICT in the belief that it enables students to learn in a multitude of different and powerful ways with great efficiency.

Educational Purpose

The College network, web sites, email and electronic learning systems have been implemented with educational imperatives in mind. All College ICT facilities and devices should only be used for educational purposes.

The Role of Students

Students are responsible for their own behaviour and actions. They are careful and respectful when using College ICT facilities and devices and only use them for the purpose of education. Students are also cyber smart and take reasonable precautions to avoid online dangers, as outlined on the Cybersmart website (www.cybersmart.gov.au). Specifically they are familiar with:

- avoiding unwanted contact;
- cyberbullying;
- trusting online friends;
- digital footprints;
- offensive content;
- identity theft.

The Role of Parents/Guardians

Parents and Guardians are ultimately responsible for setting and conveying the standards that their children should follow. The College expects that those standards will be in accordance with College rules, this policy and other College policies.

The Role of Teachers

Teachers will embrace student use of ICT in the belief that it enables students to become more powerful and efficient learners. They will provide guidance and instruction to students regarding appropriate use.

The Role of the College

The College undertakes a commitment to implement and uphold the **Student ICT Acceptable Use Policy** and to provide appropriate physical and financial resources to enable safe and educationally relevant access to ICT.

Unacceptable Use

Students should only use College ICT facilities and devices for the purpose of enhancing their education. When using ICT, students should be aware of the issues relating to privacy of both themselves and others. Students should take the utmost care when using ICT equipment as it is easily damaged and expensive to replace. Explicitly students should not:

- capture or distribute voice recordings, still images or moving footage of any person without their permission;
- create or distribute offensive messages;
- post personal details about themselves or others in electronic public spaces;
- share their user name or password with others;
- attempt to enter any area of the College network/intranet to which they do not have access rights;
- use proxy internet websites to access web content that has been restricted by the College;
- access or possess offensive material;
- play internet based games without permission.

Please note the College prohibits student use of any form of portable wireless device, apart from the College owned netbooks, on the College network.

Disciplinary Actions

Generally, pastoral teachers will ensure that appropriate consequences are put in place for inappropriate student behaviour.



Catholic College Sale

Student Information Communication Technologies (ICT) Essential Competency Checklist

Netbook computers are powerful learning tools. In order to make adequate use of the netbook it is essential that students are able to:

- ☐ recharge the netbook computer;
- ☐ use their username and password to utilise their netbook computer, College network, email and My Classes pages;
- ☐ change their password(s) regularly;
- ☐ download files from the College network via the J: Drive (public area);
- ☐ upload files to the College network via J: Drive (public area);
- ☐ create a logical file and folder structure within both their netbook computer and their personal section of the collage network – Y: Drive (private area);
- ☐ regularly back up their data on to a an external hard drive or other form of secondary storage;
- ☐ manage the Internet Explorer 'proxy settings' to enable access at home and at the College;
- ☐ use internet search engines efficiently and effectively to source information.

2 – Features of the Acer Aspire One Netbook

A considerable amount of time was invested into determining which general type and exact make of portable wireless device would best meet the needs of students at Catholic College Sale. Size, durability, battery life, price and performance were seen to be the crucial aspects.

2.1 – General specifications

The netbook that has been issued to you is an excellent machine.

Acer Aspire One Netbook

CPU: Intel Atom 1.7GHz

Memory: 2 Gb

Storage: 160 Gb

Battery: 8 hour battery life

Screen: 10.1'

Weight: 1 kg

2.2 – Preloaded software

The Windows XP operating system has been installed on to your netbook along with over fifty application software programs. Below is a list of some of the software that has been installed.

- 2007 Microsoft Office
 - Word
 - Excel
 - PowerPoint
 - Access
 - Publisher
 - Outlook
- Internet Explorer 8
- McAfee (antivirus software)
- Adobe Reader 9
- Audacity
- Photo Story 3
- Movie Maker

3 – Personalising your netbook

3.1 – Identification tag and label

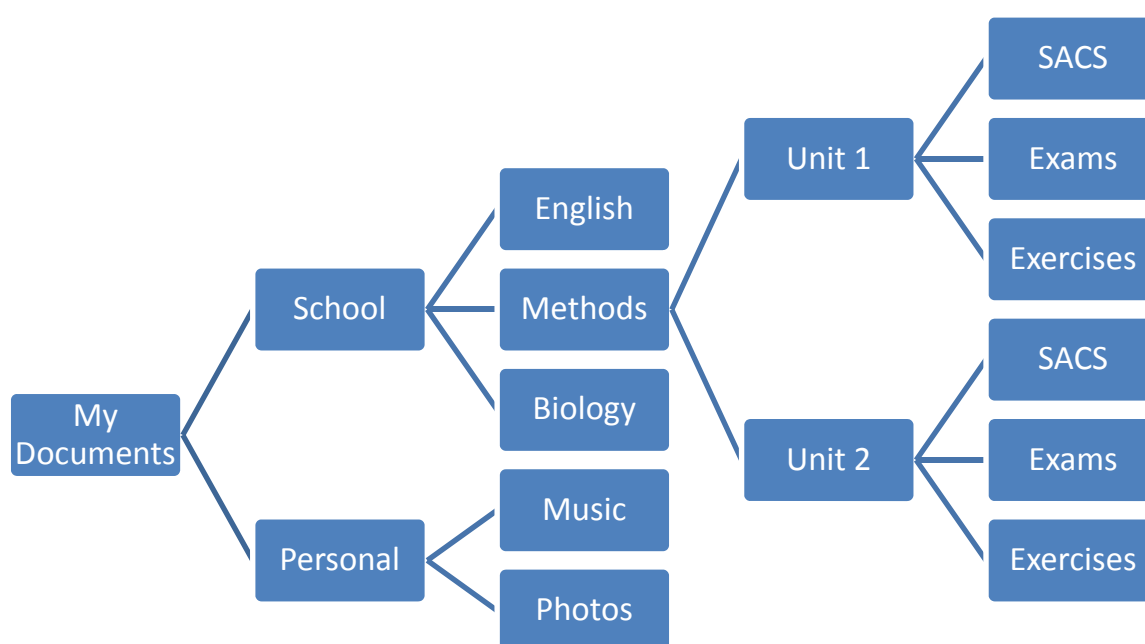
Given that all Yr 9&11 students will be issued with identical netbooks in identical protective cases it will be difficult to distinguish whose netbook is whose. For this reason you are encouraged to attach a unique tag to your case and place a small sticker on the front lid of the machine. All bags and netbooks have been added to the O'Connor Resource Centre database. The netbook and protective case that has been issued to yourself has already been loaned out in your name.

3.2 – Logging in for the first time

You will need to be on the College network when you log into your netbook for the first time. You will be unable to log in to your netbook away from the College until you have successfully logged into it whilst at school.

3.3 – Creating a logical file structure

Now is a good time to establish a sound and logical folder/file structure on your netbook. Names should be short and meaningful.



3.4 – Backing up your data

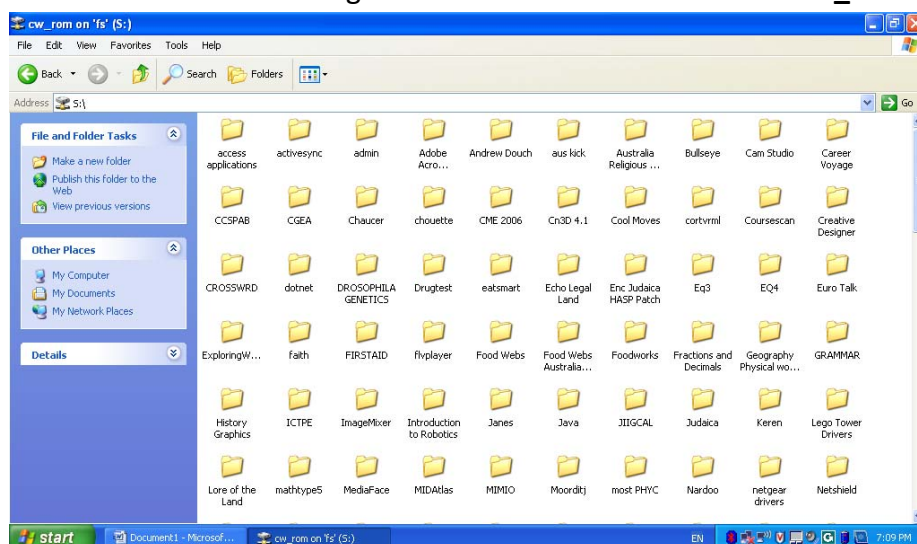
It is absolutely critical that you back up your data regularly – at least weekly! Apart from the possibility that your hard drive may fail or your netbook is stolen, the ICT Support Centre will not have the time to extensively troubleshoot the problem. Instead hard drives will be wiped clean of all data and software reloaded in a process known as re-imaging.

The most convenient and reliable way of backing up data is to make a direct copy of it into a secondary storage area such as a USB memory stick or external hard drive. If your My Documents folder consists of predominantly Microsoft Office files then it should be easily copied onto a USB memory stick. You should not pay any more than \$30 for a 8GB USB memory stick. If your My Documents folder consists of a large number of media files such as photographs and video then you should back your files up on to an external hard drive. Currently 250 GB external hard drives sell for around \$80.

3.5 – Installing additional software

Although your netbook comes with a wide range of powerful software, there will be times when new software will need to be installed. The actual process of installing software is quite easy – simply activate the set up wizard and follow the steps. However, accessing the software files with a netbook is more problematic given there is no CD/DVD drive. Software files can be downloaded directly from websites or copied across from a flash disk, external hard drive or the College network. A USB external CD/DVD drive may be borrowed from the ICT Support Centre for software files that are stored on a CD.

Software files on the College network will be located on the **CW_ROM (S:) Drive**.



Note: You are allowed to load software onto your netbook so long as it is used for educational purposes.

3.6 – Installing printers

In a lot of cases to install a home printer you simply just need to plug in the USB cable and Windows XP will automatically allow it to work (known as 'plug and play'). In some cases you may have to download particular files from the manufacturers website (refer to manufacturers user manual).

When at school your teachers will increasingly encourage you to publish information in electronic formats. However, on occasions when a hardcopy is necessary you will be able to send jobs to the printer in the O'Connor Resource Centre. This printer will be automatically installed when you log on to the network.

3.7 – Setting up Outlook (optional – limited technical support available)

You have probably been using the web based My Mail to access your school email account. Microsoft Outlook is a powerful piece of software that allows you to efficiently deal with email and schedule meetings.

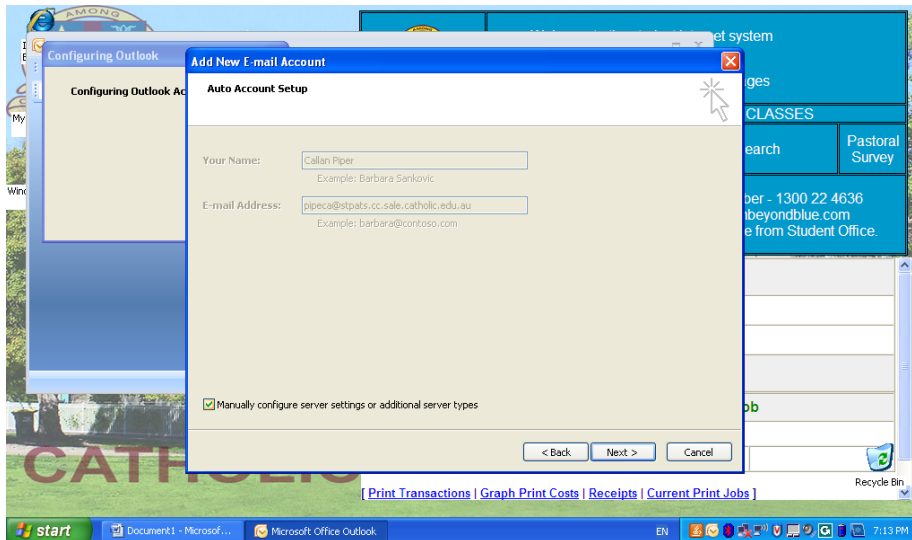
Step 1:

Select **Start > E-mail Microsoft Office Outlook** to activate the **Outlook 2007 Start Up Wizard**.



Step 2:

Select **Next > Yes > Next**. Enter in all of your details and then select **Manually configure > Next**.

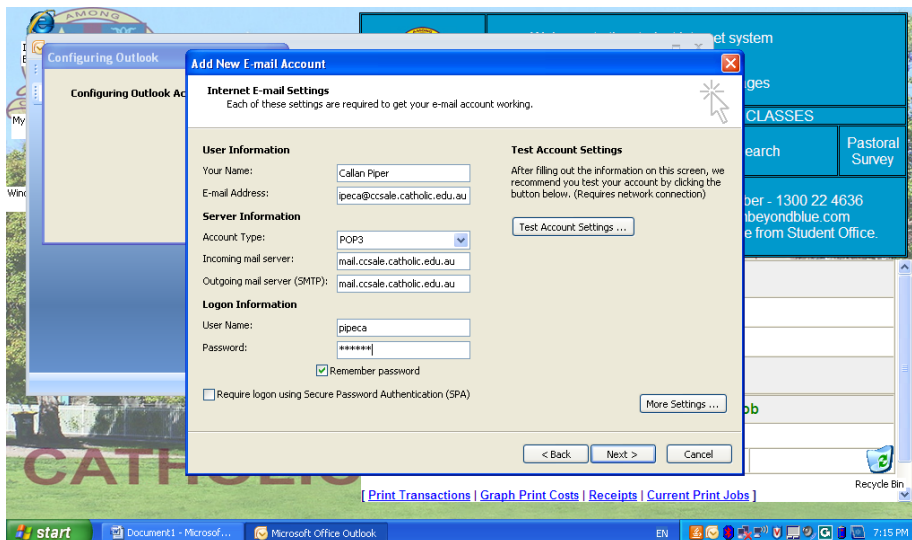


Step 3:

Select **Internet E-mail > Next**. At the **Add New E-Mail Account** enter in your personal **User Information** and **Logon Information**. It is essential that the **Server Information** is set to:

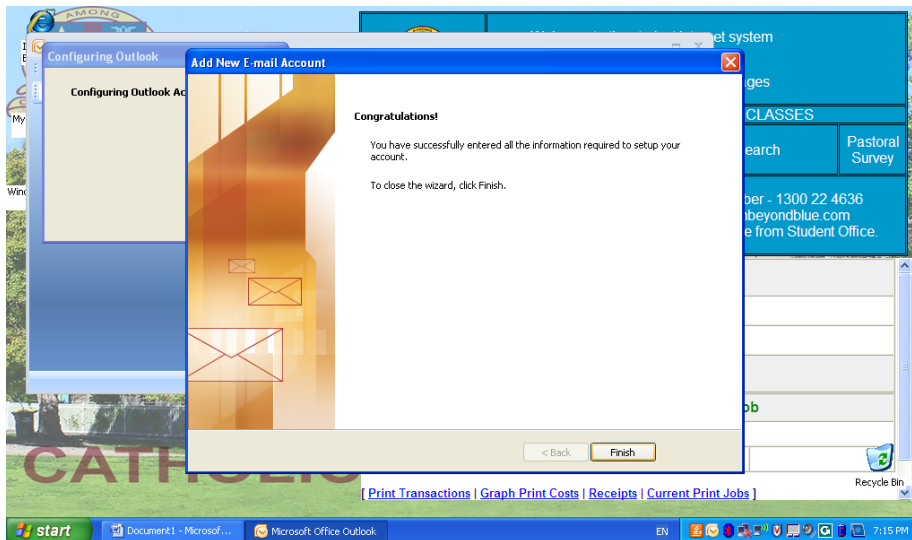
Account type:	POP3
Incoming mail server:	mail.ccsale.catholic.edu.au
Outgoing mail server (SMTP):	mail.ccsale.catholic.edu.au

Ensure that **Remember password** is selected



Step 4:

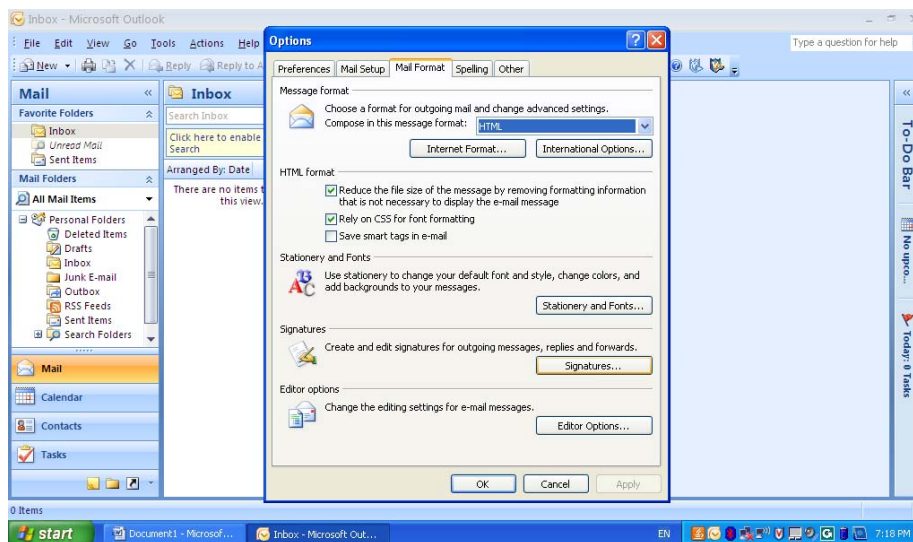
Select **Test Account Settings > Close > Finish**.



More than likely you will have the same information at the end of each email message that you compose. Rather than typing in the same information each time it is possible to create a automated signature.

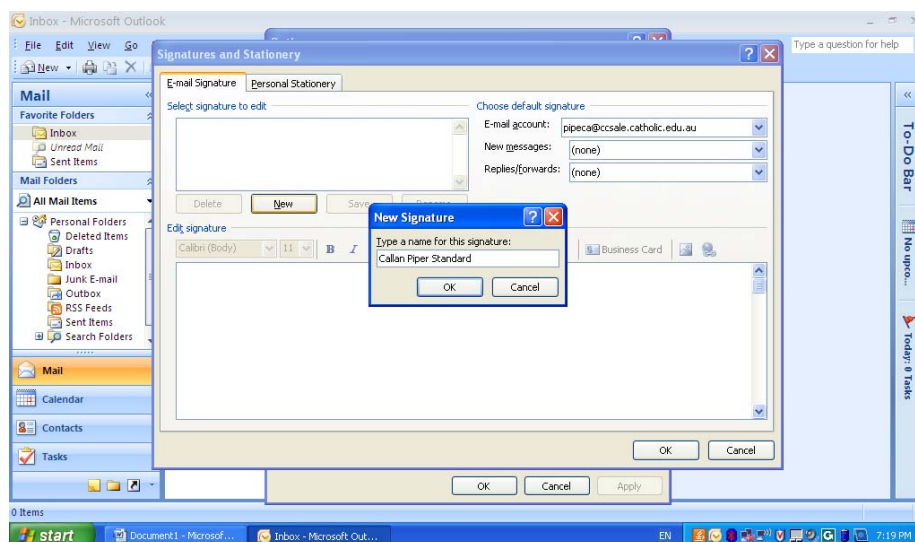
Step 5:

Open **Outlook**. Select **Tools > Options > Mail Format > Signatures**



Step 6:

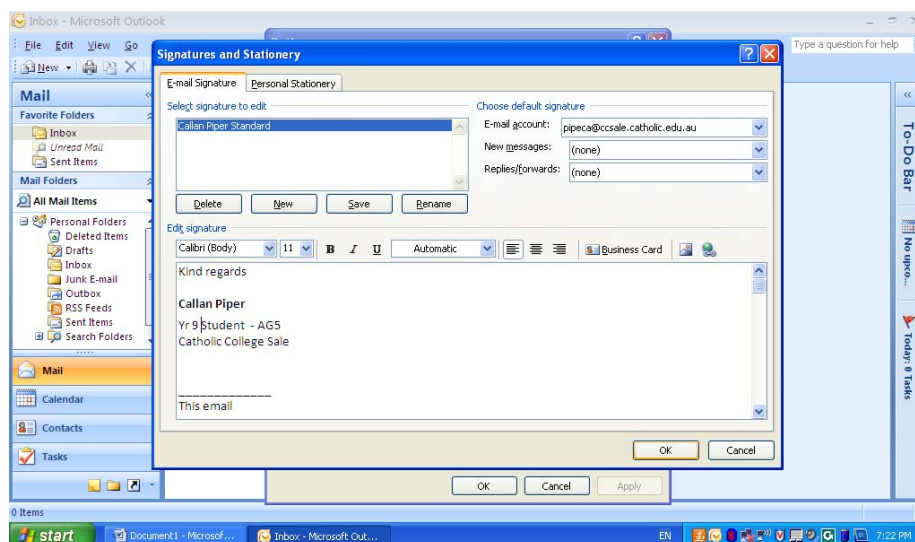
Select **New** > enter a suitable name > **OK**.



Step 7:

Enter the text for your signature. Be sure to include the following disclaimer at the very end.

This email and any attachments may be confidential. You must not disclose or use the information in this email if you are not the intended recipient. If you have received this email in error, please notify us immediately and delete the email and all copies. The College does not guarantee that this email is virus or error free. The attached files are provided and may only be used on the basis that the user assumes all responsibility for any loss, damage or consequence resulting directly or indirectly from the use of the attached files, whether caused by the negligence of the sender or not. The content and opinions in this email are not necessarily those of the College.



Select **OK** > **OK** to save the signature.

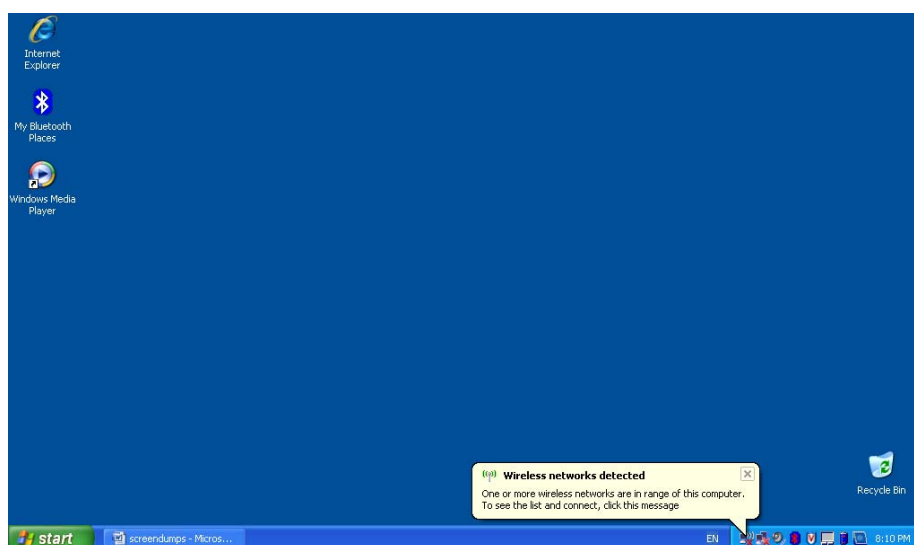
You may wish to experiment various stationary sets to alter the appearance of the email messages that you compose. Select **Tools > Options > Mail Format > Stationary and Fonts**.

3.8 – Changing your settings for use at home

To use Outlook and Internet Explorer at home a few minor settings will need to be changed. An Internet connection will also need to be established. Your Internet Service Provider will support you in establishing a connection. The steps below show how to establish a Internet connection with a wireless Telstra BigPond stationary modem and how to configure Outlook and Internet Explorer for this type of connection.

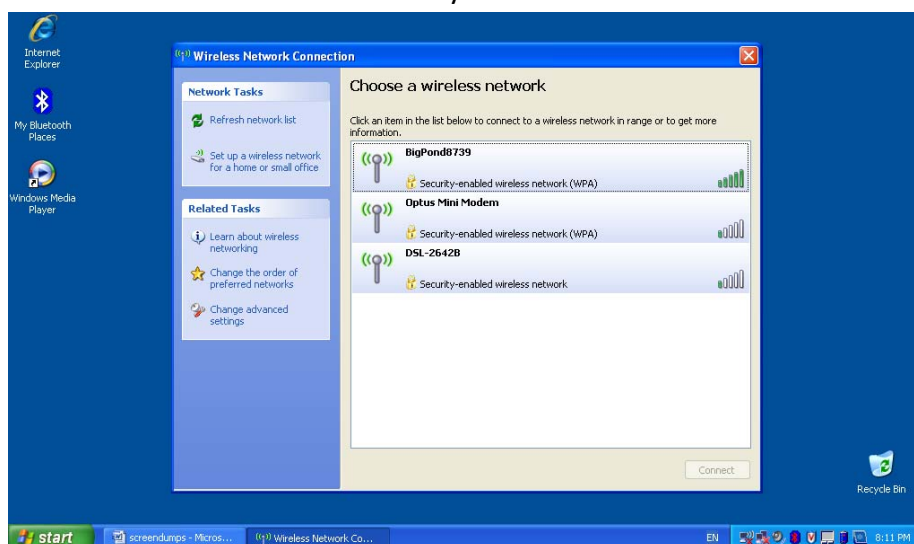
Step 1:

When you log in to your netbook, if you are in range of the wireless modem, you will see an alert message appear in the bottom right hand corner. Double click on this message.



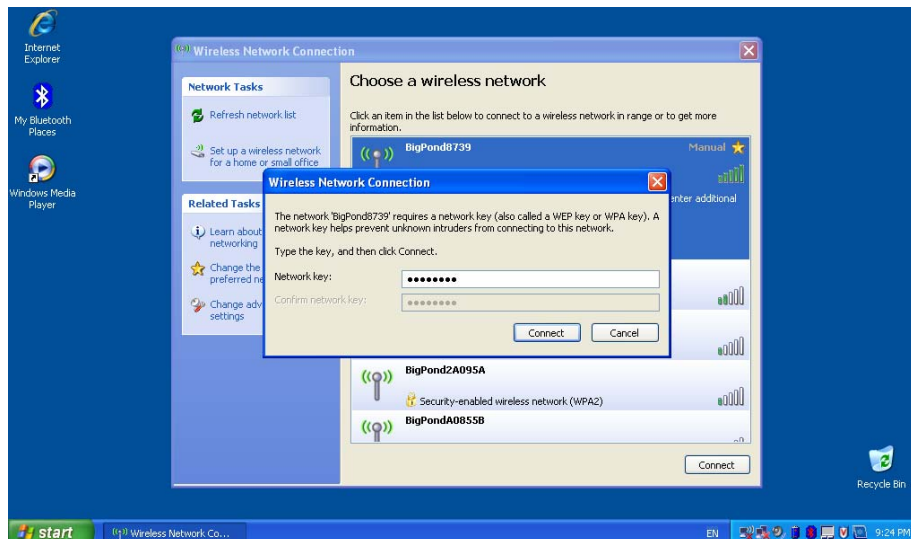
Step 2:

Choose the wireless network that you would like to connect to and then select **Connect**.



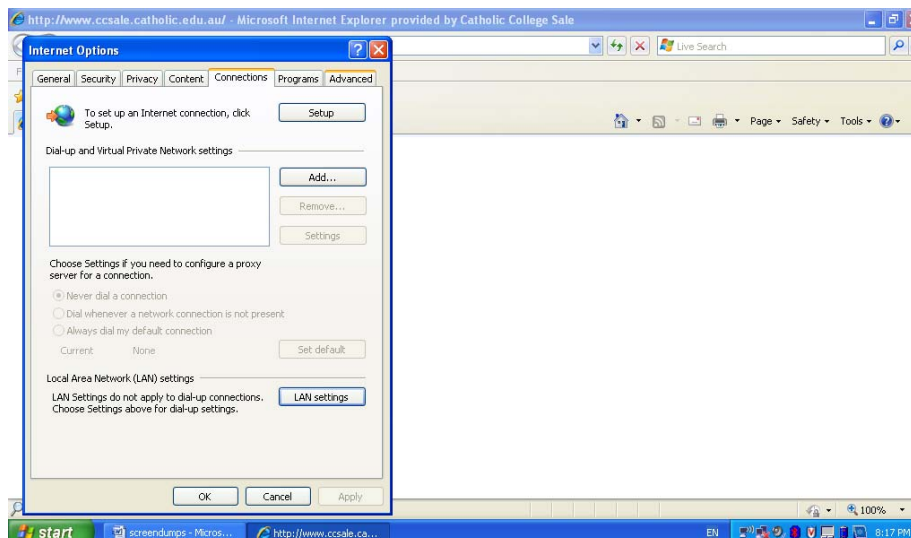
Step 3:

Enter the **Network Key** and select **Connect** to establish a connection. For a BigPond wireless account the Network Key can be found on the back of the stationary modem. It is the 10 digit number found next to **WPA:**. The Network Key will only need to be entered the first time that you establish a connection.



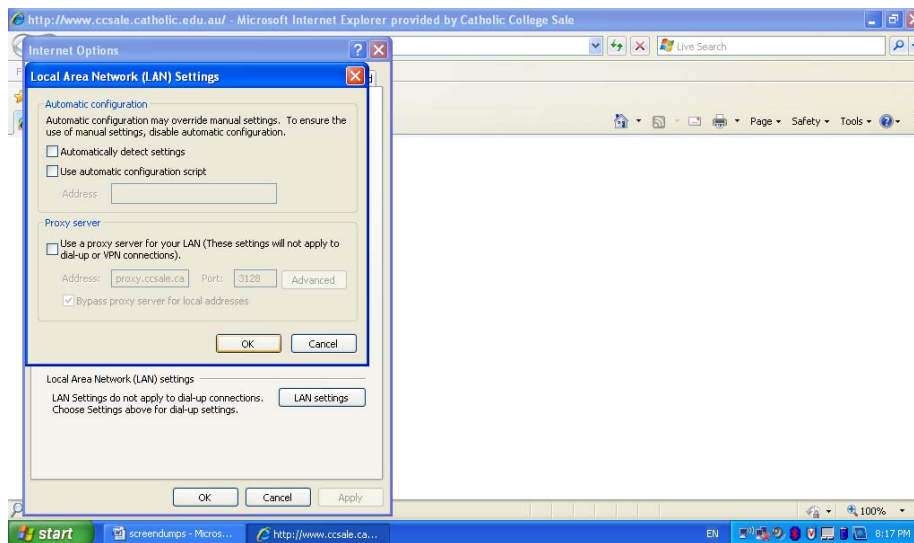
Step 4:

Open **Internet Explorer** and select **Tools > Internet Options > Connections > LAN Settings**.



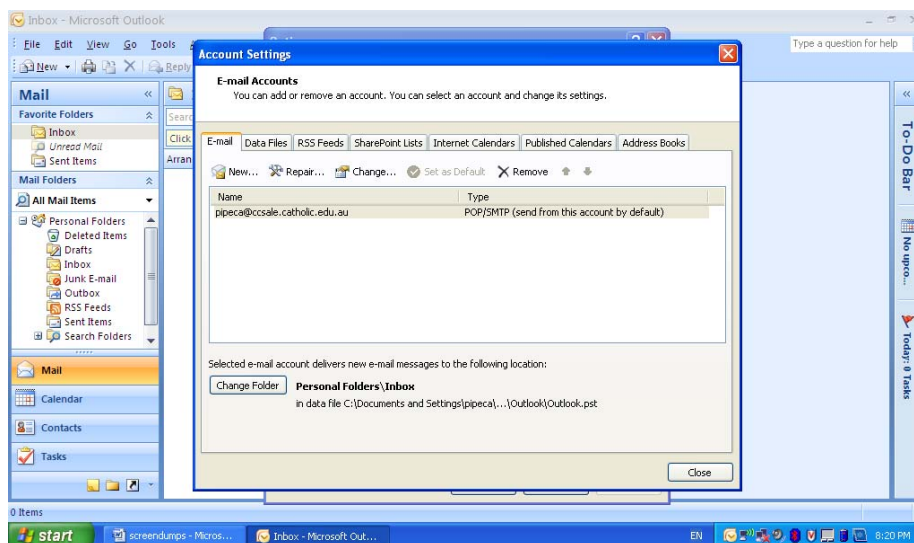
Step 5:

Uncheck the **Use a proxy server for your LAN** and then select **OK > OK**. Note this will need to be reversed to use the Internet on the College network.



Step 6:

Open **Outlook** and select **Tools > Options > Mail Set Up > E-mail Accounts**.

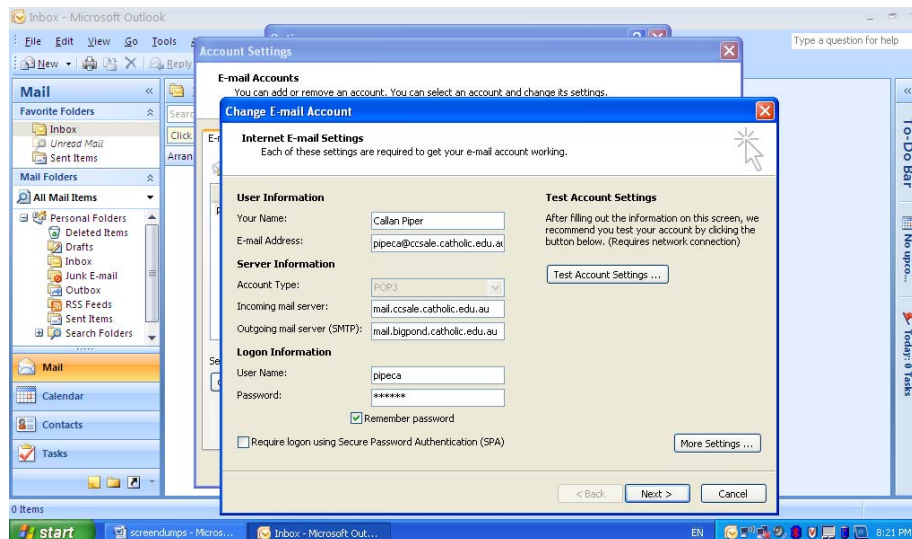


Step 7:

Double click on the email account. Within the **Server Information** section change the **Outgoing mail server (SMTP)**: so that it is set to:

Outgoing mail server (SMTP): mail.bigpond.com.au

Select **Next > Finish > Close > OK** to finalise the change.



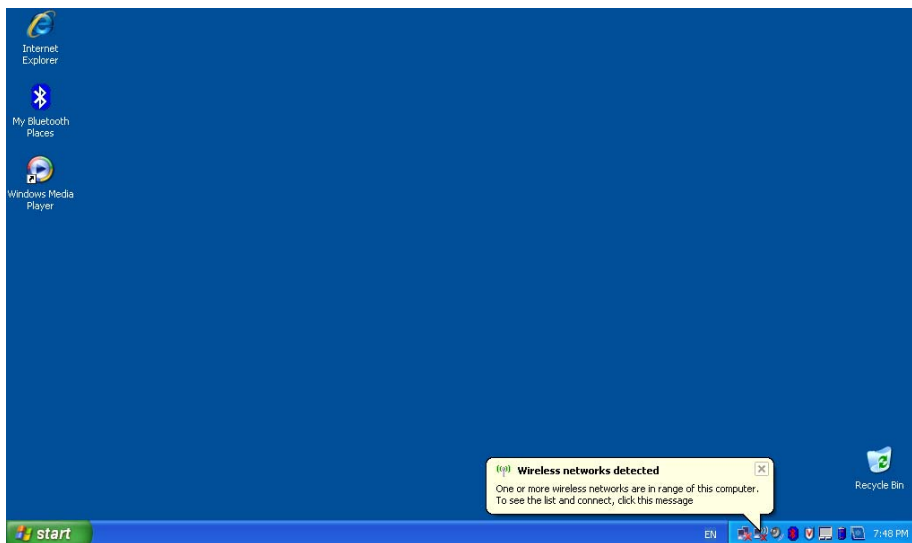
Note: Only the outgoing mail server details need to be changed. The address for the mail server will vary depending on which Internet Service Provider you use. When on the College network the above change will need to be reversed.

3.9 – Making use of Wi-Fi hotspots

Wi-Fi hotspots are public areas where people are able to establish an Internet connection with their electronic device. Public libraries and McDonald's restaurants commonly provide free wireless access to the Internet. Motels and caravan parks usually charge to provide access. The steps below outline how to access the Internet via a McDonald's Wi-Fi Hotspot.

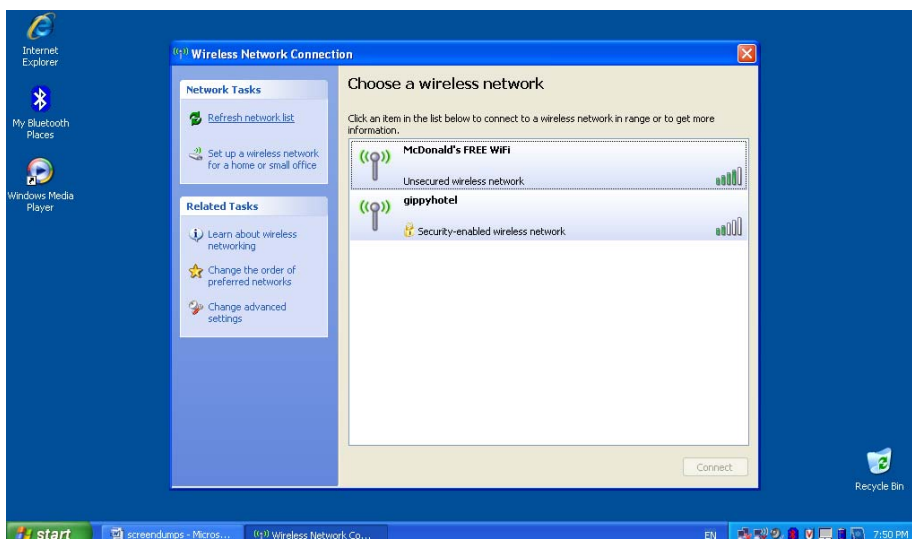
Step 1:

When you log in to your netbook, whilst in the restaurant, you will see an alert message appear in the bottom right hand corner. Double click on this message.



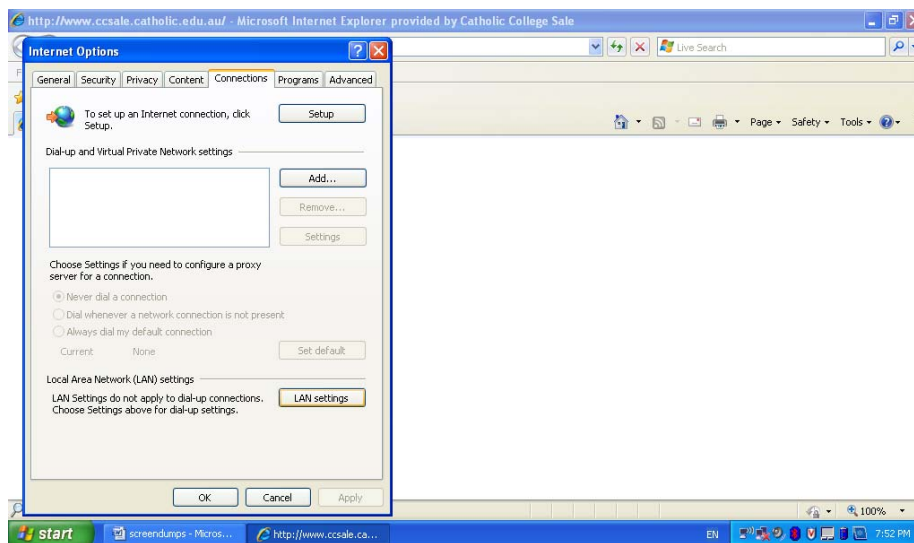
Step 2:

Choose the **McDonald's Free Wi-Fi** network and then select **Connect**.



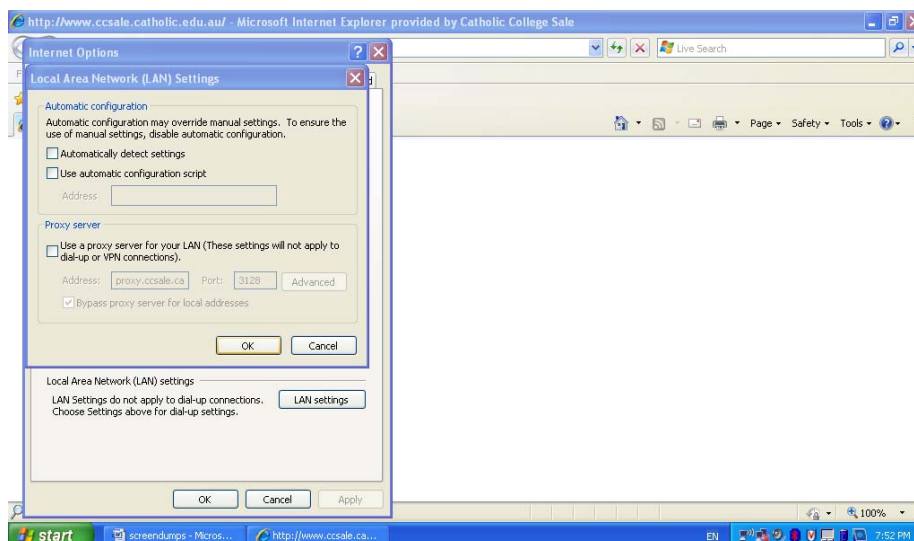
Step 3:

Open **Internet Explorer** and select **Tools > Internet Options > Connections > LAN Settings**.



Step 4:

Uncheck the **Use a proxy server for your LAN** and then select **OK > OK**. Note this will need to be reversed to use the Internet on the College network.



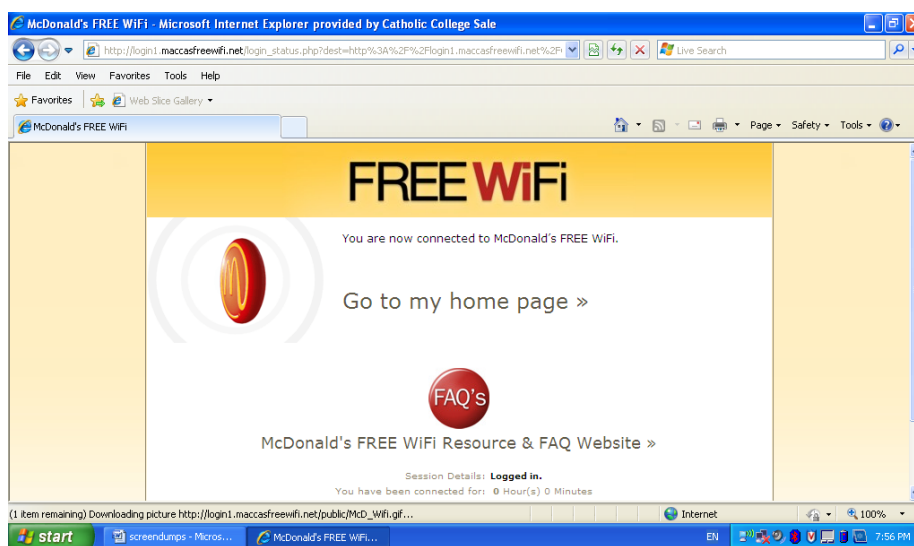
Step 5:

You will automatically be directed to the McDonald's Free Wi-Fi log in webpage. Read the terms and conditions and click on the **Click to Log in** hyperlink.

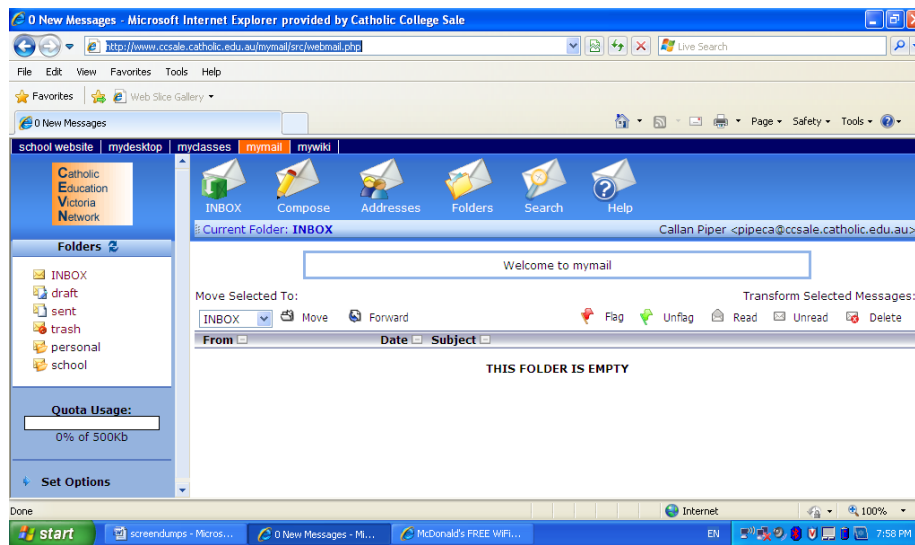


Step 6:

Click on the **Go to my home page** to be directed to the home page that you have set in Internet Explorer (usually the College home page).



Please note you will be unable to use Outlook to send email whilst using a Wi-Fi hotspot. You will need to use web based My Mail to access your account (www.ccsale.catholic.edu.au/mymail).



4 – Taking care of your netbook.

As a student, you are responsible for care of the netbook. You shall at all times take responsible care of the netbook and not expose it to undue risk of damage or theft.

4.1 – Transporting and storage

When transporting the netbook it should be carried in the protective case provided. The power pack used to recharge the netbook should never be placed with the netbook into the protective case. Jamming the power pack and the netbook together into the protective case greatly increases the chances of damaging the screen.

4.2 – Recharging the battery

You have a high quality battery installed in your netbook that should last for 8 hours before needing to be recharged. At no stage during the school day will you be given an opportunity to recharge your netbook. For these reasons there is no need to bring your power pack to school. Students should recharge their netbook each night to ensure that it is ready to be used for the following full school day.

4.3 – Cleaning your netbook

From time to time you may need to clean your netbook. At no stage should you spray your netbook with any kind of chemical. Always use a dry lint free cloth. Gently wipe the keyboard and screen to remove any dust and grime. A more thorough cleaning process will be conducted by the technicians in the ICT Support Centre towards the end of each year as part of annual maintenance.

4.4 – Seeking support

When encountering a difficulty with your netbook you should seek information from:

1. relevant sections of this manual;
2. the ICT section of the College website (www.ccsale.catholic.edu.au/ict);
3. email enquiry (netbook@ccsale.catholic.edu.au);
4. the ICT Support Centre (located in the back of K2).

In time the ICT section of the College website will contain a Q&A section that will address any issues relating to student netbooks.

5 – Cybersafety

Cybersafety refers to the protection of children when they are using ICT devices that are connected to the Internet or a telecommunications network (e.g. mobile phone, netbook or desktop computer). The information from within this section has been extracted from the federal government's cybersmart website (www.cybersmart.gov.au). Parents and students should invest a considerable amount of time digesting the contents of this site.

During the year teachers at the College will be guiding students through various programs relating to Cybersafety.

5.1 – Cyberbullying

Cyberbullying occurs when the internet, email or mobile phones are used to deliberately and repeatedly engage in hostile behaviour to harm someone. Cyberbullying can result in those involved experiencing social, psychological and academic difficulties. Children can cyberbully each other in a number of ways. These include:

- sending abusive text or emails
- posting unkind messages or inappropriate images on social networking sites
- imitating others online
- excluding others online.

Children and young people can also be affected by hostile behaviour that is not cyberbullying. For example, a one off insensitive or negative remark or joke posted online, or sent by text, may not be considered cyberbullying, however it can still have a negative impact on a child.

Tips for parents to help their teenage children deal with cyberbullying.

Talk to your teen about cyberbullying before it happens. Work out strategies to address cyberbullying that you are both comfortable with, so your child knows what to expect if they do report concerns to you or another trusted adult. Reassure them that you will be there to support them and won't disconnect them from their online world.

Encourage your teen to tell you or another trusted adult if they receive or hear of negative messages, or are excluded by others. Help them stay connected to trusted friends and family both online and offline. This is an important protective measure against the potentially negative outcomes of bullying.

Advise your teen not to respond to any negative messages but to save the messages and details of the senders. You may want to save the messages for your teen so that they don't keep reading them and potentially feel worse.

You can help your teen report any concerns to the administrator of the service used, including the mobile phone provider (if SMS is involved), website administrator (if social networking or chat services are involved), or internet service provider.

Encourage your teen to support their friends and report concerns about friends who may be involved in cyberbullying.

Advise your child never to share their password with friends—friendships may be shortlived at this age and former friends can misuse passwords to cyberbully.

If your child has been involved in cyberbullying and seems distressed or shows changes in behaviour or mood it may be advisable to seek professional support, including through the Cybersmart Online Helpline at www.cybersmart.gov.au/report.aspx. The Cybersmart Online Helpline provides free, confidential online counselling for children and young people.

Note: Students can seek guidance from their Pastoral Teacher, House Leader or make an appointment, via the Student Office, with the School Counsellor.

5.2 – Sexting

Sexting refers to the sending of provocative or sexual photos, messages, or videos, generally using a mobile phone. It can also include posting this type of material online.

While sharing suggestive images or text messages may seem like innocent flirting or be funny for young people, sexting can have serious social and legal consequences. To help protect their image both online and offline, young people need to consider how they manage their own and others' messages and images.

Tips for parents to help their teenage sons and daughters deal with sexting.

Talk with your teen about sexting and the social and legal consequences it can have.

Sexting can have legal consequences if the images taken and shared are of minors. Even if all participants are willing, teens may be breaking the law if they take and share naked or sexual images of themselves or others who are minors. This is because sexting images may be considered child pornography.

Sexting can have social consequences. For example, if images are forwarded on from the intended recipient, which has been the case following relationship break-ups, the social ramifications can be devastating for teens. Images may end up being viewed by many people through mobiles and posting of images online.

Remind your teen to delete any sexual content they receive from others and to avoid forwarding this type of content.

Remind your teen to consider the feelings of others when taking photos and distributing any content by mobile phone or online.

If you are concerned that a sexting incident may be a criminal matter, contact your local police.

If your teen is exposed to inappropriate content or involved in creating such content talk with them about it. If necessary seek professional support, including support through the Cybersmart Online Helpline at <http://www.cybersmart.gov.au/report.aspx>. The Cybersmart Online Helpline provides free, confidential online counselling for children and young people.

Note: Students can seek guidance from their Pastoral Teacher, House Leader or make an appointment, via the Student Office, with the School Counsellor.

5.3 – Online grooming

Children and young people can communicate with people online who they don't know, or have not met, in real life. While being in contact with new people can be exciting, the anonymity offered by the internet can allow these new contacts to cover their true identities. For example, someone who says they are a 10 year-old girl could actually be a 40 year-old man. This anonymity means that sexual solicitation and online grooming can occur online and are serious risks.

Sexual solicitation is where someone is asked to engage in a sexual conversation or activity or to send a sexually explicit image or information.

Online grooming and procuring of children over the internet is the illegal act of an adult or adults making online contact with a child under the age of sixteen with the intention of facilitating a sexual relationship. More information is available from the Australian Federal Police which investigates suspected cases of online grooming.

Tips for parents to help their teenage sons and daughters deal with online grooming.

Stay involved in your teen's use of new technologies—keep up to date with the websites they are visiting and explore them with your teen if possible. In general it is useful to consider whether you are comfortable with the content of the sites and the potential for contact with others including adults.

Remind your teen to create screen names or IDs that do not indicate gender, age, name or location and are not sexually provocative.

Guide your teen to use their privacy settings to restrict their online information to viewing by known friends only.

Encourage your teen to keep their online friends online. If they want to meet someone that they haven't met in person encourage them to ask a parent or another trusted adult to go with them and always meet in public places, preferably during the day.

Encourage your teen to be alert to people online who make them feel uncomfortable and to block them. They should report inappropriate contact to the website administrators.

Some teens feel worried about their parents' reaction to things they may have said or done online, especially if they think they encouraged online sexual contact. This can prevent them reporting concerns about online contacts. Perpetrators play on this worry and shame to isolate teens from family and friends and encourage teens to trust and confide in them.

To overcome this risk reassure your teen that you will always support them and not block their internet access if they report that they are uncomfortable or worried about what somebody has been saying online.

Be alert to changes in your teen's behaviour or mood that are concerning including increased or decreased sexualised behaviours and/or apparent confidence, clinginess or withdrawal, anxiety or sadness and changed interactions with friends. Explore your concerns with them and if necessary seek professional support including through the Cybersmart Online Helpline at www.cybersmart.gov.au/report.aspx. The Cybersmart Online Helpline provides free, confidential online counselling for children and young people.

Note: Students can seek guidance from their Pastoral Teacher, House Leader or make an appointment, via the Student Office, with the School Counsellor.

5.4 – Protecting personal information

Personal information is any information that identifies an individual. Personal information includes full name, address, date of birth, phone numbers, email addresses, usernames and passwords, bank details, student identity card details or passport details.

Online, personal information is used by many businesses to verify a user's identity. While personal information can be safely disclosed to many legitimate businesses, if not managed carefully, it can be accessed and misused by criminals. It can also be used by marketers who may send spam through email or SMS.

Disclosing personal information online can also impact on a user's 'digital reputation'. A Digital reputation is the opinion that others hold about people based on what they do and say online.

Tips for parents to help their teenage sons and daughters deal with protecting personal information.

Remind your teen that not everyone is who they claim to be. Although they may enjoy having many online friends, adding people that they don't know on 'friends lists' allows those people to learn all about them. This information could be used for scams, to steal their identity or worse.

Talk to your teen about managing personal information on social networking sites. Encourage them not to put any personal information on their profiles. This includes their phone number, personal email address, home or school addresses, or the name of their school.

Encourage your teen to be careful when they post photos that they are not accidentally providing clues to personal information such as their school uniform.

Encourage your teen to set up a separate email account for use when signing up to games or websites. This account will be separate to all other personal accounts so they can disable it if it's misused. It should not include their names or other identifiers in the address.

They might also like to set up a separate social networking account if they want to promote themselves or an interest and engage with like minded people that they don't know offline. They should ensure the site does not contain their personal information.

Encourage your teen to read user agreements and privacy policies to determine how their personal information may be used when signing up to services as many organisations use information for their own marketing and some sell it to other marketing firms.

Remind your teen that they should only disclose financial information on websites that they trust and that have secure payment facilities identified by a web address beginning with <https://> and a 'locked' padlock symbol in the bottom of the screen, which indicates that data is being encrypted.

Remind your teen that banking institutions will never email individuals asking for their user name or password. If they receive an email from an organisation claiming to represent a banking institution they should report the email to the bank and the Government's SCAMwatch website at www.scamwatch.gov.au or their local consumer affairs agency. They should not respond and not click on any links provided.

5.5 – Excessive internet usage

To many parents it seems as though children and young people are constantly online. Often they seem to be completing more than one task at a time; for example, downloading and listening to music while studying and chatting with friends or sending messages on their mobile phones.

The number of hours children and young people spend online can vary significantly. There is no guideline for the 'right' amount of time for children to spend online, however if their online behaviour appears to impact negatively on their behaviour or wellbeing, or that of the family, it may be time to discuss expectations and establish time limits.

Tips for parents to help their teenage sons and daughters deal with excessive internet usage.

Look for indicators that your teen may be spending too much time online, such as a decline in interest in other activities, talking constantly about an online game or activity, a decline in grades or irritability when they are away from a game. You may also suspect they are getting up after bed time to play games or chat to others.

Teens may seem quite tired during the day or skip meals to avoid leaving the computer.

If issues arise consider establishing rules about when teens can play games or use the internet and how long they can play each day. You might consider agreeing with your teen a set balance of online and offline activities. You may need to establish consequences for rule breaches. For example, if your teen doesn't undertake their assigned jobs they may have access to online games restricted.

Try to locate the computer in a shared or visible place in the home so you are aware of how much time your teen spends online.

If you have concerns about your teen's online behaviour explore your concerns with them. If necessary seek professional support, including support through the Cybersmart Online Helpline at www.cybersmart.gov.au/report.aspx. The Cybersmart Online Helpline provides free, confidential online counselling for children and young people.

Note: Students can seek guidance from their Pastoral Teacher, House Leader or make an appointment, via the Student Office, with the School Counsellor.